JOURNAL OF NUMBER THEORY **14**, 315–326 (1982)

# The Rank of Group of Cyclotomic Units in Abelian Fields

KEQIN FENG

*Chinese University of Science and Technology, Hofei, Anhui, The People's Republic of China*

*Communicated by H. Zassenhaus*

Received July 11, 1980

A formula about the rank of group of cyclotomic units in abelian fields is established. From that formula, a series of equivalent conditions for independence of the system of cyclotomic units in abelian fields is stated and proved. For the particular case of cyclotomic fields, further properties of the rank are researched.

## 1. INTRODUCTION

Let $m \geqslant 5$ be a natural number. $\zeta_m = e^{2\pi i/m}$. If $m = p^l$ and $p$ is an odd prime, it is well known since Kummer that

$$\left\{ \frac{1-\zeta_{p_l}^{g^{i+1}}}{1-\zeta_{p_l}^{g^i}} \mid 1 \leqslant i \leqslant \frac{\varphi(p^l)}{2} - 1 \right\}$$

is an independent system of cyclotomic units, where $g$ is a primitive root mod $p^l$. If $m$ is a composite number, we know that

$$\mathscr{E}_h = \frac{1-\zeta_m^h}{1-\zeta_m}, \qquad (h, m) = 1, \quad 2 \leqslant h < \frac{m}{2}, \tag{1}$$

are units in cyclotomic field $\mathbb{Q}(\zeta_m)$. There are many mathematicians who are interested in the multiplicative relations of these units (e.g., [1, 4]). Particularly, is the system of cyclotomic units (1) independent? Ramachandra [4] gave examples of $m$ for which system (1) is not independent. Pei and Feng [3] gave a necessary and sufficient condition for independence of system (1) and, after that, we found all $m$ such that system (1) is independent system in the field $\mathbb{Q}(\zeta_m)$ (see Sction 3, Theorem 4 of this paper). As a matter of fact, Hasse [2] has already studied this problem for general abelian fields.



0022-314X/82/030315-12$02.00/0

Let $K/\mathbb{Q}$ be a finite abelian extension. According to the Kronecker–Weber Theorem, $K$ is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_m)$. The least natural number $m$ satisfying this property is called the conductor of the abelian field $K$ and expressed by $\mathrm{cond}(K)$.

Galois group $G(\mathbb{Q}(\zeta_m)/K)$ is a subgroup of $G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ which can be considered as $\mathbb{Z}_m^*$ (reduced class group mod $m$). So $G(\mathbb{Q}(\zeta_m)/K$ can be considered as a subgroup $H$ of $\mathbb{Z}_m^*$ and Galois group $G = G(K/\mathbb{Q})$ as the quotient group $\mathbb{Z}_m^*/H$.

It is easy to see that $|\mathbb{Z}_m^*/(\pm H)| = r + 1$ where $r$ is the rank of unite group of $K$. Let $h_0 = 1, h_1, \ldots, h_r$ be a completely representative system of $\mathbb{Z}_m^* (\mathrm{mod}\ \pm H)$ and consider the set of cyclotomic units of $K$

$$\mathscr{E} = \{\varepsilon_{h_i} \mid 1 \leqslant i \leqslant r\}, \qquad \varepsilon_h = N_{\mathbb{Q}(\zeta_m)/K}\left(\frac{1-\zeta_m^h}{1-\zeta_m}\right).$$

Hasse proved

THEOREM (Hasse [2, p. 19]). *Suppose that $K/\mathbb{Q}$ is an abelian extension of degree $n$. For any rational prime $p$ we have the decomposition into prime ideal in $K$*

$$p = (\mathscr{P}_1 \cdots \mathscr{P}_{g_p})^{e_p}, \qquad e_p f_p g_p = n.$$

*Then $\mathscr{E}$ is an independent system of units in $K$ if and only if $g_p = 1$ for any rational prime divisor $p$ of* $\mathrm{cond}(K)$.

In this paper I will give a formula about the rank of group of cyclotomic units for arbitrary abelian field (Section 2). Particularly for cyclotomic fields I will study further properties of this rank. Since $\mathscr{E}$ is independent for the case $\mathrm{cond}(K) = p^l$, from now on we assume that $m$ is a composite number.

## 2. A FORMULA OF RANK OF GROUP OF CYCLOTOMIC UNITS

As above, let $K/\mathbb{Q}$ be an abelian extension of degree $n$. $\mathrm{Cond}(K) = m$ is a composite number (so $m \not\equiv 2 \pmod 4$). $G = G(K/\mathbb{Q}) \cong \mathbb{Z}_m^*/H$. Let $K^+$ be the maximal real subfield of $K$. Then $G(K^+/\mathbb{Q}) \cong \mathbb{Z}_m^*/(\pm H)$.

Using terminology in the theory of class fields, a character of field $K^+$ means a character of its Galois group $G^+ = G(K^+/\mathbb{Q}) \cong \mathbb{Z}_m^*/(\pm H)$. Such character corresponds obviously an even character mod $m$ which acts trivially on $H$. Suppose that $\chi$ is arbitrary non-trivial character of $K^+$. Let

$$S_m(\chi) = \sum_{\pm x (\mathrm{mod}\ m)} \chi(x)(-\log|1-\zeta_m^x|)$$

$$= \sum_{x \in \mathbb{Z}_m^* (\mathrm{mod}\ \pm H)} \chi(x) \sum_{x \in H} (-\log|1-\zeta_m^x|)$$

$$= \sum_{x \in \mathbb{Z}_m^* (\mathrm{mod}\ \pm H)} \chi(x)(-\log|N_{\mathbb{Q}(\zeta_m)/K}(1-\zeta_m^x)|)$$

$$= \sum_{x \in \mathbb{Z}_m^* (\mathrm{mod}\ \pm H)} \chi(x)(-\log|\varepsilon_x|).$$

According to Hasse [2] we have

$$\text{(I)} \quad S_m(\chi) = \prod_{p|m} (1-\chi(p)) \cdot S_{f(\chi)}(\chi), \tag{2}$$

where $f(\chi)$ is the conductor of $\chi$ and

$$S_{f(\chi)}(\chi) = \sum_{\pm x (\mathrm{mod}\ f(\chi))} \chi(x)(-\log|1-\zeta_{f(\chi)}^x|).$$

(II) (formula of class number of real abelian fields)

$$h^+ R^+ = \prod_{\chi \neq 1} S_{f(\chi)}(\chi).$$

The sum is taken for all non-trivial characters $\chi$ of $K^+$ and $R^+$ is the regulator of $K^+$. Particularly, we have

$$S_{f(\chi)}(\chi) \neq 0 \tag{3}$$

for any non-trivial character $\chi$ of $K^+$.

A completely representative system of $\mathbb{Z}_m^* (\mathrm{mod}\ \pm H)$, $h_0 = 1, h_1, \ldots, h_r$ are considered as all elements of group $G(K^+/\mathbb{Q})$. In this way we look at the Frobenius group matrix

$$M = (-\log|\varepsilon_{h_i h_j^{-1}}|)_{0 \leqslant i,j \leqslant r}.$$

It is easy to see that the maximal number of multiplicatively independent units in $\mathscr{E}$ equals to the maximal number of independent columns in $M$, i.e.,

$$\mathrm{rank}(E_0) = \mathrm{rank}(M), \tag{4}$$

where $E_0 = E_0(k)$ denotes the group of cyclotomic units of $K$ generalized by $\mathscr{E}$. Let $\chi_0 = 1, \chi_1, \ldots, \chi_r$ be all characters of $K^+$. Using the orthogonal relations between these characters

$$\sum_{j=0}^{r} \bar{\chi}_k(h_j)\chi_l(h_j) = (r+1)\delta_{kl}.$$

We know that the matrix

$$P = (\bar{\chi}_j(h_i))_{0 \leqslant i,j \leqslant r}$$

have inverse matrix

$$P^{-1} = \frac{1}{r+1}(\chi_i(h_j)).$$

Thus,

$$P^{-1}MP = D = (d_{ij}),$$

where

$$\begin{aligned} d_{ij} &= \frac{1}{r+1} \sum_{k,l=0}^{r} \chi_i(h_k)(-\log|\varepsilon_{h_k h_l^{-1}}|)\chi_j(h_l) \\ &= \frac{1}{r+1} \sum_{k=0}^{r} \chi_i(h_k) \sum_{l=0}^{r} (-\log|\varepsilon_{h_k h_l^{-1}}|)\chi_j(h_l^{-1}h_k)\bar{\chi}_j(h_k) \\ &= \frac{1}{r+1} \sum_{t=0}^{r} (-\log|\varepsilon_{h_t}|)\chi_j(h_t) \sum_{k=0}^{r} \chi_i(h_k)\bar{\chi}_j(h_k) \\ &= \delta_{ij} \sum_{t=0}^{r} (-\log|\varepsilon_{h_t}|)\chi_j(h_t). \end{aligned}$$

Therefore, $P^{-1}MP = \operatorname{diag}\{d_0, d_1, \ldots, d_r\}$, where

$$d_i = \sum_{t=0}^{r} \chi_i(h_t)(-\log|\varepsilon_{h_t}|) = \sum_{x \in Z_m^*(\bmod \pm H)} \chi_i(x)(-\log|\varepsilon_x|) = S_m(\chi_i).$$

From that and formulas (2), (3) and (4) we obtain the following lemma.

LEMMA 1.

$$\operatorname{rank}(E_0) = \#\{i \mid 1 \leqslant i \leqslant r,\ d_i \neq 0\} = \#\left\{i \mid 1 \leqslant i \leqslant r,\ \prod_{p \mid m}(1 - \chi_i(p)) \neq 0\right\}.$$

Particularly, we get several necessary and sufficient conditions for independence of $\mathscr{E}$ as following

LEMMA 2. *For a finite abelian field $K$ following statements are equivalent to each other.*

(1) *the system $\mathscr{E}$ of cyclotomic units of $K$ is independent;*

(2) $\sum_{t=0}^{r} \chi(h_t)(-\log|\varepsilon_{h_t}|) \neq 0$ *for any non-trivial even character $\chi$ of $K$;*

(3) $\chi(p) \neq 1$ *for any non-trivial even character* $\chi$ *of* $K$ *and any prime divisor* $p$ *of* $m = \mathrm{cond}(K)$.

Now we deduce a more explicit formula for $\mathrm{rank}(E_0)$ from which we can get another equivalent condition for independence of $\mathscr{E}$. Let

$$m = p_1^{\alpha_1} \cdots p_l^{\alpha_l}.$$

Then we have the natural isomorphism

$$\mathbb{Z}_m^* \cong \prod_{i=1}^{l} \mathbb{Z}_{p_i^{\alpha_i}}^*, \qquad a \pmod m \mapsto (a \pmod{p_1^{\alpha_1}}, \ldots, a \pmod{p_l^{\alpha_l}}).$$

For any set of subscripts $I = \{i_1, \ldots, j_\lambda\}$, $1 \leqslant i_1 < i_2 < \cdots < i_\lambda \leqslant l$, consider the projective mapping

$$\mathbb{Z}_m^* = \prod_{i=1}^{l} \mathbb{Z}_{p_i^{\alpha_i}}^* \xrightarrow{\rho} \mathbb{Z}_{m/p_{i_1}^{\alpha_{i_1}} \cdots p_{i_\lambda}^{\alpha_{i_\lambda}}}^*, \qquad (a_1, \ldots, a_l \mapsto (b_1, \ldots, b_l),$$

where

$$\begin{aligned} b_i &= 1 \qquad \text{for} \quad i = i_1, \ldots, i_\lambda \\ &= a_i \qquad \text{otherwise.} \end{aligned}$$

At last, let

$$H_I = H_{i_1, \ldots, i_\lambda} = \rho(H).$$

THEOREM 1. *Let* $\langle \pm H_{i_1, \ldots, i_\lambda}, p_{i_1}, \ldots, p_{i_\lambda} \rangle$ *denote the subgroup of* $\mathbb{Z}_{m/p_{i_1}^{\alpha_{i_1}} \cdots p_{i_\lambda}^{\alpha_{i_\lambda}}}^*$ *generated by* $\pm H_{i_1, \ldots, i_\lambda}, p_{i_1}, \ldots, p_{i_\lambda}$ *and*

$$n_I = n_{i_1, \ldots, i_\lambda} = [\mathbb{Z}_{m/p_{i_1}^{\alpha_{i_1}} \cdots p_{i_\lambda}^{\alpha_{i_\lambda}}}^* : \langle \pm H_{i_1, \ldots, i_\lambda}, p_{i_1}, \ldots, p_{i_\lambda} \rangle].$$

*Then*

$$\begin{aligned} \mathrm{rank}(E_0(K)) &= (r+1) + \sum_{k=1}^{l} (-1)^k \sum_{\substack{I \subset \{1, \ldots, l\} \\ |I| = k}} n_I = (r+1) - \sum_{i=1}^{l} n_i \\ &\quad + \sum_{1 \leqslant i < j \leqslant l} n_{ij} - \cdots + (-1)^l n_{12 \ldots l} \\ &= r - \sum_{k=1}^{l-1} (-1)^k \sum_{\substack{I \subset \{1, \ldots, l\} \\ |I| = k}} (n_I - 1). \end{aligned}$$

*Proof.* As we said before, a character $\chi$ of $K^+$ is of its Galois group

$\mathbb{Z}_m^*/(\pm H)$ or a character mod $m$ which acts trivially on $(\pm H)$. According to Lemma 1,

$$\begin{aligned}\operatorname{rank}(E_0(K)) &= \#\{i \mid 1 \leqslant i \leqslant r, \prod_{p \mid m} (1-\chi_i(p)) \neq 0\} \\ &= \#\{i \mid 1 \leqslant i \leqslant r, \chi_i(p_j) \neq 1 \qquad (1 \leqslant j \leqslant l)\}. \end{aligned} \tag{5}$$

Let $\chi$ be arbitrary character of $K^+$. For $1 \leqslant i_1 < i_2 < \cdots < i_\lambda \leqslant l$ we define

$$M_{i_1,\ldots,i_\lambda} = \{\chi \mid \chi \text{ is a character of } K^+, \chi(p_{i_1}) = \chi(p_{i_2}) = \cdots = \chi(p_{i_\lambda}) = 1\}.$$

If $\chi \in M_{i_1,\ldots,i_\lambda}$, then $p_{i_j} \nmid f(\chi)$ $(1 \leqslant j \leqslant \lambda)$. Thus, $\chi$ can be considered as a character mod $m/p_{i_1}^{\alpha_{i_1}} \cdots p_{i_\lambda}^{\alpha_{i_\lambda}}$ and acts trivially on subgroup $\langle \pm H_{i_1,\ldots,i_\lambda}, p_{i_1},\ldots,p_{i_\lambda}\rangle$. According to the dual theorem we have

$$|M_{i_1,\ldots,i_\lambda}| = [\mathbb{Z}^*_{m/p_{i_1}^{\alpha_{i_1}}\cdots p_{i_\lambda}^{\alpha_{i_\lambda}}} : \langle \pm H_{i_1,\ldots,i_\lambda}, p_{i_1},\ldots,p_{i_\lambda}\rangle] = n_{i_1,\ldots,i_\lambda}. \tag{6}$$

Using formulas (5) and (6), the definition of set $M_{i_1,\ldots,i_\lambda}$ and the inclusion–exclusion principle we get the formula of $\operatorname{rank}(E_0(K))$ in the theorem.

*Remark.* Since the rank of unit group $E$ of $K$ is $r$, Theorem 1 can be restated as

$$\operatorname{corank}(E_o(K)) = \sum_{k=1}^{l-1} (-1)^{k-1} \sum_{\substack{I \subset \{1,\ldots,l\} \\ |I|=k}} (n_I - 1). \tag{7}$$

COROLLARY. *Suppose that $K$ is an abelian field,* $\operatorname{cond}(K) = m = p_1^{\alpha_1} p_2^{\alpha_2}$ $(\alpha_1, \alpha_2 \geqslant 1)$. *Then*

$$\operatorname{corank}(E_0(K)) = g(p_1, K^+/\mathbb{Q}) + g(p_2, K^+/\mathbb{Q}) - 2,$$

*where $g(p, K^+/\mathbb{Q})$ denotes the number of $K^+$ prime divisors of $p$.*

*Proof.* From the formula of corank (5) we know that

$$\operatorname{corank}(E_0(K)) = n_1 + n_2 - 2.$$

Thus it is enough to prove that $g(p_i, K^+/\mathbb{Q}) = n_1$ $(i = 1, 2)$. For doing that let $K_1$ denote the maximal unramified subfield of $K^+$ for $p_1$. Then $G(K_1/\mathbb{Q}) \cong \mathbb{Z}^*_{p_2^{\alpha_2}/(\pm H_1)}$ and

$$g(p_1, K+/\mathbb{Q}) = g(p_1, K_1/\mathbb{Q}) = \left[ G(K_1/\mathbb{Q}) : \left\langle \left( \frac{K_1/\mathbb{Q}}{p_1} \right) \right\rangle \right],$$

where $(K_1/\mathbb{Q}/p_1)$ is the Frobenius automorphism of extension $K_1/\mathbb{Q}$ at $p_1$. But the right-hand side equals

$$[\mathbb{Z}^*_{p_2^{\alpha_2}/(\pm H_1)}: \langle p_1 \rangle] = [\mathbb{Z}^*_{p_2^{\alpha_2}}: \langle \pm H_1, p_1 \rangle] = n_1$$

i.e., $g(p_1, K^+/\mathbb{Q}) = n_1$. With the same reason we have $g(p_2, K^+/\mathbb{Q}) = n_2$.

From Theorem 1 we can get new equivalent conditions for independence of $\mathscr{E}$ as following condition (5) and (6).

THEOREM 2. *Suppose that $K$ be an abelian field and* $\mathrm{cond}(K) = m = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$. *Then the following statements are equivalent to each other.*

(1) *The system $\mathscr{E}$ of cyclotomic units of $K$ is independent*;

(4) $\mathbb{Z}^*_{m/p_i^{\alpha_i}} = \langle \pm H_i, p_i \rangle \quad (1 \leqslant i \leqslant l)$;

(5) (Hasse) $g(p, K^+/\mathbb{Q}) = 1$ *for any prime divisor $p$ of $m$.*

*Proof.* (1) $\Leftrightarrow$ (4). We know that condition (1) is equivalent to condition (3) in Lemma 2 which can be restated as following

$$(3') \quad \chi_i(p_j) \neq 1 \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant l),$$

where $\chi_0 = 1$, $\chi_1, \ldots, \chi_r$ are characters of $K^+$. But by the dual theorem we have

$$\#\{\chi_i \mid 1 \leqslant i \leqslant r, \chi_i(p_j) = 1\} = [\mathbb{Z}^*_{m/p_j^{\alpha_j}}: \langle \pm H_j, p_j \rangle] - 1 \qquad (1 \leqslant j \leqslant l).$$

Thus,

$$(3') \Leftrightarrow [\mathbb{Z}^*_{m/p_j^{\alpha_j}}: \langle \pm H_j, p_j \rangle] = 1 \qquad (1 \leqslant j \leqslant l),$$

i.e., (1) and (4) are equivalent.

(4) $\Leftrightarrow$ (5). Let $K_i$ denote the maximal unramified subfield of $K^+$ for $p_i$. Then $G(K_i/\mathbb{Q}) \cong \mathbb{Z}^*_{m/p_i^{\alpha_i}}/(\pm H_i)$. Using the same argument as in the proof of the corollary of Theorem 1, we have

$$g(p_i, K^+/\mathbb{Q}) = g(p_i, K_i/\mathbb{Q}) = \left[G(K_i/\mathbb{Q}): \left\langle \left(\frac{K_i/\mathbb{Q}}{p_i}\right) \right\rangle\right] = [\mathbb{Z}^*_{m/p_i^{\alpha_i}/(\pm H_i)}: \langle p_i \rangle]$$

$$= [\mathbb{Z}^*_{m/p_i^{\alpha_i}}: \langle \pm H_i, p_i \rangle] \qquad (1 \leqslant i \leqslant l).$$

Therefore conditions (4) and (5) are equivalent. So we proved Hasse's theorem in the Introduction with a little different way from Hasse's original proof.

## 3. The Case of Cyclotomic Fields

Now we restrict things into the case of cyclotomic fields and give some further discussion. In this case Theorems 1 and 2 can be restated as follows.

THEOREM 3. *Let* $m = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ $(l \geqslant 2)$, $\alpha_i \geqslant 1$ $(1 \leqslant i \leqslant l)$, $m \not\equiv 2 \pmod 4$ *and*

$$\mathscr{E} = \left\{ \varepsilon_h = \frac{1-\zeta_m^h}{1-\zeta_m} \;\middle|\; (h, m) = 1,\ 2 \leqslant h < m/2 \right\}.$$

*If* $E_0(m)$ *denotes the group of cyclotomic units of* $\mathbb{Q}(\zeta_m)$ *generated by* $\mathscr{E}$. *Then*

$$(1)\quad \operatorname{rank}(E_0(m)) = \frac{\varphi(m)}{2} + \sum_{k=1}^{l} (-1)^k \sum_{\substack{I \subset \{1,\ldots,l\} \\ |I| = k}} n_I$$

$$= \left( \frac{\varphi(m)}{2} - 1 \right) + \sum_{k=1}^{l-1} (-1)^k \sum_{\substack{I \subset \{1,\ldots,l\} \\ |I| = k}} (n_I - 1),$$

*where*

$$n_I = n_{i_1,\ldots,i_\lambda} = \left| \mathbb{Z}^*_{m/p_{i_1}^{\alpha_{i_1}} \cdots p_{i_\lambda}^{\alpha_{i_\lambda}}} : \langle -1, p_{i_1}, \ldots, p_{i_\lambda} \rangle \right|$$

*for* $I = \{i_1, \ldots, i_\lambda\}$, $1 \leqslant i_1 < i_2 < \cdots < i_\lambda \leqslant l$.

(2) (Pei and Feng [3]). *The system* $\mathscr{E}$ *of cyclomatic uits of field* $\mathbb{Q}(\zeta_m)$ *is independent if and only if*

$$\mathbb{Z}^*_{m/p_i^{\alpha_i}} = \langle -1, p_i \rangle \qquad (1 \leqslant i \leqslant l). \tag{8}$$

Using the condition (8), Pei and Feng [3] determined all the values of $m$ for which the system $\mathscr{E}$ is independent in the field $\mathbb{Q}(\zeta_m)$. I restate this result here for completeness. At first, if (1) $m = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$, $l \geqslant 4$, or (2) $m = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_l^{\alpha_l}$, $\alpha_0 \geqslant 3$, $l \geqslant 2$, then formula (8) cannot be satisfied for $i = l$ because in these cases $\mathbb{Z}^*_{m/p_l^{\alpha_l}}$ can be decomposed into direct product of at least three non-trivial cyclic subgroups so cannot be generated by two elements $-1$ and $p_l$. In general case, for $p \nmid n$ we define $n$ a semi-primitive root mod $p^\alpha$ if the order of $n \pmod{p^\alpha}$ is $\frac{1}{2}\varphi(p^\alpha)$. Then our result is the following.

THEOREM 4 (Pei and Feng [3]). *For composite number* $m$, *the system* $\mathscr{E}$ *of cyclotomic units of field* $\mathbb{Q}(\zeta_m)$ *is independent if and only if one of the*

*following conditions is satisfied* (*here* $\alpha_0 \geqslant 3$; $\alpha_1, \alpha_2, \alpha_3 \geqslant 1$; $p_1, p_2, p_3$ *are odd primes*):

(I) $m = 4p_1^{\alpha_1}$; *and*

(I, 1) 2 *is a primitive root* mod $p_1^{\alpha_1}$; *or*

(I, 2) 2 *is a semi-primitive root* mod $p_1^{\alpha_1}$ *and* $p_1 \equiv 3 \pmod 4$.

(II) $m = 2^{\alpha_0}p_1^{\alpha_1}$; *the order of* $p_1 \pmod{2^{\alpha_0}}$ *is* $2^{\alpha_0-2}$, $p_1^{2^{\alpha_0-3}} \not\equiv -1 \pmod{2^{\alpha_0}}$, *and*

(II, 1) 2 *is a primitive root* mod $p_1^{\alpha_1}$; *or*

(II, 2) 2 *is a semi-primitive root mod* $p_1^{\alpha_1}$ *and* $p_1 \equiv 3 \pmod 4$.

(III) $m = p_1^{\alpha_1}p_2^{\alpha_2}$; *and*

(III, 1) *when* $p_1 \equiv p_2 \equiv 3 \pmod 4$: $p_1$ *is a primitive root* mod $p_2^{\alpha_2}$ *and* $p_2$ *is a semi-primitive root* mod $p_1^{\alpha_1}$ *or vice versa.*

(III, 2) *otherwise*: $p_1$ *and* $p_2$ *are primitive root* mod $p_2^{\alpha_2}$ *and* mod $p_1^{\alpha_1}$, *respectively.*

(IV) $m = 4p_1^{\alpha_1}p_2^{\alpha_2}$; $(p_1 - 1, p_2 - 1) = 2$, *and*

(IV, 1) *when* $p_1 \equiv p_2 \equiv 3 \pmod 4$: 2 *is a primitive root for one p and a semi-primitive root for another p*; $p_1$ *is a primitive root* mod $2p_2^{\alpha_2}$ *and* $p_2$ *is a semi-primitive root* mod $2p_1^{\alpha_1}$ *or vice versa.*

(IV, 2) *when* $p_1 \equiv 1$, $p_2 \equiv 3 \pmod 4$: 2 *is a primitive root mod* $p_2^{\alpha_2}$; $p_1$ *and* $p_2$ *are primitive root* mod $p_2^{\alpha_2}$ *and* mod $p_1^{\alpha_1}$, *respectively.*

(IV, 3) *when* $p_1 \equiv 3$, $p_2 \equiv 1 \pmod 4$: *a condition similar* to (IV, 2) *but exchange the place of* $p_1$ *and* $p_2$.

(V) $m = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}$; $p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod 4$; $(p^i - 1)/2$ $(1 \leqslant i \leqslant 3)$ *are coprime to each other*; *and*

(V, 1) $p_1, p_2, p_3$ *are primitive root* mod $p_2^{\alpha_2}$, mod $p_3^{\alpha_3}$, mod $p_1^{\alpha_1}$, *respectively, and semi-primitive root* mod $p_3^{\alpha_3}$, mod $p_1^{\alpha_1}$, mod $p_2^{\alpha_2}$, *respectively*; *or*

(V, 2) $p_1, p_2, p_3$ *are primitive root* mod $p_3^{\alpha_3}$, mod $p_1^{\alpha_1}$, mod $p_2^{\alpha_2}$, *respectively and semi-primitive root* mod $p_2^{\alpha_2}$, mod $p_3^{\alpha_3}$, mod $p_1^{\alpha_1}$, *respectively.*

At the end of this paper, we give two theorems which concern the relation of corank $(E_0)$ between different cyclotomic fields.

THEOREM 5. *Suppose m and k are compositie numbers and have the same prime divisors. If* $k \mid m$, $\operatorname{corank}(E_0(\mathbb{Q}(\zeta_m))) \geqslant \operatorname{corank}(E_0(\mathbb{Q}(\zeta_k)))$.

*Proof.* From assumptions of the theorem we can write down

$$m = p_1^{\alpha_1} \cdots p_l^{\alpha_l}, \qquad k = p_1^{\beta_1} \cdots p_l^{\beta_l}, \qquad g(p_i) \leqslant \beta_i \leqslant \alpha_i \qquad (1 \leqslant i \leqslant l),$$

where $g(p)=1$ if $p\geqslant 3$ and $g(p)=2$ if $p=2$. Let $\mathbb{Q}(m)=\mathbb{Q}(\zeta_m)$, $E_0(\mathbb{Q}(\zeta_m))=E_0(m)$ briefly. For $(\lambda,p_i)=1$ we have

$$N_{\mathbb{Q}(p_i^{\alpha_i})/\mathbb{Q}(p_i^{\beta_i})}(1-\zeta_{p_i^{\alpha_i}}^{\lambda}X)=\prod_{t=0}^{p_i^{\alpha_i-\beta_i-1}}(1-\zeta_{p_i^{\alpha_i}}^{\lambda(1+tp_i^{\beta_i})}X)=(1-\zeta_{p_i^{\beta_i}}^{\lambda}X^{p_i^{\alpha_i-\beta_i}})$$

So if $\zeta_m=\zeta_{p_1^{\alpha_1}}^{\lambda_1}\cdots\zeta_{p_l^{\alpha_l}}^{\lambda_l}$, then

$$\begin{aligned}N_{\mathbb{Q}(m)/\mathbb{Q}(k)}(1-\zeta_m^h)&=N_{\mathbb{Q}(m)/\mathbb{Q}(k)}(1-\zeta_{p_1^{\alpha_1}}^{h\lambda_1}\cdots\zeta_{p_l^{\alpha_l}}^{h\lambda_l})\\&=N_{\mathbb{Q}(m/p_1^{\alpha_1})/\mathbb{Q}(k/p_1^{\beta_1})}(1-\zeta_{p_1^{\beta_1}}^{h\lambda_1}(\zeta_{p_2^{\alpha_2}}^{h\lambda_2}\cdots\zeta_{p_l^{\alpha_l}}^{h\lambda_l})^{p_1^{\alpha_1-\beta_1}})\\&=\cdots<(1-\zeta_{p_1^{\beta_1}}^{h\mu_1}\cdots\zeta_{p_l^{\beta_l}}^{h\mu_1})=(1-\zeta_k^{h\mu}),\end{aligned}$$

where

$$\mu_i=\prod_{\substack{j=1\\ j\neq 1}}^{l}p_j^{\alpha_j-\beta_j},\qquad \zeta_k^{\mu}=\zeta_{p_1^{\beta_1}}^{\mu_1}\cdots\zeta_{p_l^{\beta_l}}^{\mu_l}.$$

Since $(\mu_i,p_i)=1$ $(1\leqslant i\leqslant l)$, $(\mu,k)=1$ and

$$N_{\mathbb{Q}(m)/\mathbb{Q}(k)}\left(\frac{1-\zeta_m^h}{1-\zeta_m}\right)=\frac{1-\zeta_k^{h\mu}}{1-\zeta_k^{\mu}}\qquad(2\leqslant h<k/2,\ (h,k)=1)\tag{9}$$

are cyclotomic units of $\mathbb{Q}(k)$. The unit group generated by system (9) has the same corank as the group $E_0(k)$. For any $u$ independent multiplicative relations between cyclotomic units (9)

$$\prod_h\left|\frac{1-\zeta_k^{h\mu}}{1-\zeta_k^{\mu}}\right|^{\alpha_{hj}}=1\qquad(1\leqslant j\leqslant u),\qquad \alpha_{hj}\in\mathbb{Z}$$

we get

$$\begin{aligned}1&=N_{\mathbb{Q}(m)/\mathbb{Q}(k)}\left(\prod_h\left|\frac{1-\zeta_m^h}{1-\zeta_m}\right|^{\alpha_{hj}}\right)\\&=\prod_h\left|\frac{1-\zeta_m^h}{1-\zeta_m}\right|^{\alpha_{hj}}\prod_h\prod_{\substack{\sigma\in(\mathbb{Q}(m)/\mathbb{Q}(k))\\ \sigma\neq 1}}\left(\left|\frac{1-\sigma(\zeta_m^h)}{1-\zeta_m}\right|^{\alpha_{hj}}\left|\frac{1-\sigma(\zeta_m)}{1-\zeta_m}\right|^{-\alpha_{hj}}\right).\end{aligned}$$

$$(1\leqslant j\leqslant u)\tag{10}$$

It is easy to see that when $(h,\sigma)\neq(h',\sigma')$, $2\leqslant h$, $h'<k/2$, $(h,k)=(h',k)=1$, $\sigma$, $\sigma'\in G(\mathbb{Q}(m)/\mathbb{Q}(k))$, we have $|1-\sigma(\zeta_m^h)|\neq|1-\sigma'(\zeta_m^{h'})|$. Thus, formula (10) can be considered as $u$ multiplicative relations between cyclotomic units in $\mathbb{Q}(m)$ and they are independent. Thus, we proved that $\operatorname{corank}(E_0(m))\geqslant\operatorname{corank}(E_0(k))$.

For $l$ different primes $p_1, p_2, \ldots, p_l$ we let

$$S = \{p_1^{\alpha_1} \cdots p_l^{\alpha_l} \mid \alpha_i \geqslant g(p_i) \qquad (1 \leqslant i \leqslant l)\},$$

$$\mathbb{Q}(S) = \{\mathbb{Q}(\zeta_m) \mid m \in S\},$$

where $g(p_i) = 1$ for $p_i \geqslant 3$ and $g(p_i) = 2$ for $p_i = 2$. From Theorem 5 we know that when $M \supset K$, $M, K \in \mathbb{Q}(S)$ then $\operatorname{corank}(E_o(M)) \geqslant \operatorname{corank}(E_0(K))$. On the other hand, when $l = 2$ we shall prove that for any fixed prime pair $\{p_1, p_2\}$, the $\operatorname{rank}(E_0)$ of all fields in $\mathbb{Q}(S)$ are bounded above. For doing that let $O_{p^\alpha}(n)$ denote the order of $n \pmod{p^\alpha}$ where $p \nmid n$. It is trivial that $O_{p^{\alpha+1}}(n) = O_{p^\alpha}(n)$ or $p \cdot O_{p^\alpha}(n)$. Let

$$f_p(n) = \min\{\alpha \mid \alpha \geqslant g(p), O_{p^{\alpha+1}}(n) = p \cdot O_{p^\alpha}(n)\}.$$

THEOREM 6. *Suppose* $m = p_1^{\alpha_1} p_2^{\alpha_2}$, $\alpha_i \geqslant g(p_i)$ $(i = 1, 2)$, $f_1 = f_{p_1}(p_2)$, $f_2 = f_{p_2}(p_2)$, $m_0 = p_1^{f_1} p_2^{f_2}$:

(1) *Let* $K = \mathbb{Q}(\zeta_{p_2^{\alpha_2}})$. *Then for cyclotomic* $p_1$*-adic extension of* $k$

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots, \qquad K_n = K\mathbb{Q}(\zeta_{p_1^n}),$$

*we have* $\operatorname{corank}(E_0(K_{f_1})) = \operatorname{corank}(E_0(K_{f_1+1})) = \cdots$.

(2) *If* $m_0 \mid m$, *then* $\operatorname{corank}(E_0(\mathbb{Q}(\zeta_m))) = \operatorname{corank}(E_0(\mathbb{Q}(\zeta_{m_0})))$.

*Proof.* At first we claim that $(n, p) = 1$ and $O_{p^{\alpha+1}}(n) = p \cdot O_{p^\alpha}(n)$ for some $\alpha \geqslant g(p)$, then it is also right for $\alpha + 1$. In fact, let $\lambda = O_{p^\alpha}(n)$, then from this assumption we know that $n^\lambda = 1 + lp^\alpha$, $(l, p) = 1$. Thus $n^{\lambda p} \equiv 1 + lp^{\alpha+1} \not\equiv 1 \pmod{p^{\alpha+2}}$, i.e., $O_{p^{\alpha+2}}(n) = p \cdot O_{p^{\alpha+1}}(n)$.

Now we are going to prove (1). Let $\lambda = O_{p_1^{f_1}}(p_2)$. From the above claim and the definition of $f_1$ we get $O_{p_1^{f_1+t}}(p_2) = \lambda \cdot p_1^t$. Thus

$$[\mathbb{Z}^*_{p_1^{f_1+t}} : \langle -1, p_2\rangle] = \frac{\varphi(p_1^{f_1+t})}{\lambda \cdot p_1^t} = \frac{\varphi(p_1^{f_1})}{\lambda} \qquad \text{if} \quad p_1 \geqslant 3 \quad \text{and} \quad 2 \mid \lambda$$

$$= \frac{\varphi(p_1^{f_1+t})}{2\lambda p_1^t} = \frac{\varphi(p_1^{f_1})}{2\lambda} \qquad \text{otherwise}$$

$$= [\mathbb{Z}^*_{p_1^{f_1}} : \langle -1, p_2\rangle].$$

According to the formula of $\operatorname{corank}(E_0)$ we get

$$\begin{aligned}\operatorname{corank}(E_0(K_t)) &= [\mathbb{Z}^*_{p_1^{f_1+t}} : \langle -1, p_2\rangle] - 1 + [\mathbb{Z}^*_{p_2^{\alpha_2}} : \langle -1, p_1\rangle] - 1 \\ &= [\mathbb{Z}^*_{p_1^{f_1}} : \langle -1, p_2\rangle] - 1 + [\mathbb{Z}^*_{p_2^{\alpha_2}} : \langle -1, p_1\rangle] - 1 \\ &= \operatorname{corank}(E_0(K_0)) \qquad (t = 1, 2, \ldots)\end{aligned}$$

(2) can be obtained from (1) easily.

*Remark* 1. Theorem 6(1) can be generalized a little more. Instead of $\mathbb{Q}(\zeta_{p_2^{\alpha_2}})$ we can take any subfield $K$ and get the same conclusion by slightly changing the proof.

*Remark* 2. The values of $m_0 = p_1^{f_1} p_2^{f_2}$ and $\operatorname{corank}((E_0(\mathbb{Q}(\zeta_{m_0})))$ for all $2 \leqslant p_1, p_2 \leqslant 19$ are tabulated as follows.

| $(p_1, p_2)$ | (2, 3) | (2, 5) | (2, 7) | (2, 11) | (2, 13) | (2, 17) | (2, 19) | (3, 5) |
|---|---|---|---|---|---|---|---|---|
| $m_0$ | $2^4 \cdot 3$ | $2^2 \cdot 5$ | $2^4 \cdot 7$ | $2^3 \cdot 11$ | $2^2 \cdot 13$ | $2^4 \cdot 17$ | $2^3 \cdot 19$ | $3 \cdot 5$ |
| $\operatorname{corank}(E_0(\mathbb{Q}(\zeta_{m_0})))$ | 0 | 0 | 1 | 0 | 0 | 4 | 0 | 0 |
| $(p_1, p_2)$ | (3, 7) | (3, 11) | (3, 13) | (3, 17) | (3, 19) | (5, 7) | (5, 11) | (5, 13) |
| $m_0$ | $3 \cdot 7$ | $3 \cdot 11^2$ | $3 \cdot 13$ | $3^2 \cdot 17$ | $3^2 \cdot 19$ | $5^2 \cdot 7$ | $5 \cdot 11$ | $5 \cdot 13$ |
| $\operatorname{corank}(E_0(\mathbb{Q}(\zeta_{m_0})))$ | 0 | 10 | 1 | 2 | 2 | 4 | 1 | 2 |
| $(p_1, p_2)$ | (5, 17) | (5, 19) | (7, 11) | (7, 13) | (7, 17) | (7, 19) | (11, 13) | (11, 17) |
| $m_0$ | $5 \cdot 17$ | $5 \cdot 19$ | $7 \cdot 11$ | $7 \cdot 13$ | $7 \cdot 17$ | $7^3 \cdot 19$ | $11 \cdot 13$ | $11 \cdot 17$ |
| $\operatorname{corank}(E_0(\mathbb{Q}(\zeta_{m_0})))$ | 0 | 1 | 0 | 2 | 0 | 48 | 0 | 0 |
| $(p_1, p_2)$ | (11, 19) | (13, 17) | (13, 19) | (17, 19) | | | | |
| $m_0$ | $11 \cdot 19$ | $13 \cdot 17$ | $13 \cdot 19$ | $17 \cdot 19$ | | | | |
| $\operatorname{corank}(E_0(\mathbb{Q}(\zeta_{m_0})))$ | 2 | 4 | 0 | 1 | | | | |

## REFERENCES

1. H. BASS, Generators and relations for cyclotomic units, *Nagoya Math. J.* **27** (1966), 401–407.
2. H. HASSE, Über die Klassenzahl Abelschen Zahlkörper, Berlin 1952.
3. D. Y. PEI AND K. FENG, On independence of the cyclotomic units, *Acta Math. Sinica* **23** (1980), 773–778.
4. K. RAMACHANDRA, On the units of cyclotomic fields, *Acta Arith.* **12** (1966), 165–173.